The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
02/04/2021

SUBJECT:
Multiple Vulnerabilities in SolarWinds Orion and ServU-FTP Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in SolarWinds Orion and ServU-FTP, the most severe of which could allow for remote code execution.

- SolarWinds Orion provides centralized monitoring across an organization's entire IT stack.
- ServU-FTP is a multi-protocol file server capable of sending and receiving files from other networked computers through various means.

Successful exploitation of the most severe of these vulnerabilities could result in remote code execution that allows complete control of the underlying Windows operating system. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- SolarWinds Orion Platform versions prior to 2020.2.4
- SolarWinds ServU-FTP versions prior to 15.2.2 HF1

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in SolarWinds Orion and ServU-FTP, the most severe of which could allow for remote code execution. Details of these vulnerabilities are as follows:

- The SolarWinds Orion Collector service relies heavily on Microsoft Message Queue (MSMQ), with a large list of private queues available. Unauthenticated remote users can send messages to the queues over TCP port 1801 and can execute arbitrary code due to an insecure deserialization. This could allow an attacker to gain complete control of the underlying Windows system. (CVE-2021-25274)
- Credentials for the SolarWinds Orion backend database were insufficiently protected, which allows local authenticated users to have unrestricted access to them. The sensitive data in the SOLARWINDS_ORION configuration file can be read locally by authenticated users. After authenticating to the Microsoft SQL Server with the decrypted credentials, a threat actor would have complete control over the SolarWinds Orion database and could steal information or add admin-level users. (CVE-2021-25275)
- The SolarWinds Serv-U FTP Server stores user accounts in a separate files on the disk. These files can be created by any authenticated user. By setting a simple field in the file and setting the home directory to the root of the system drive, an authenticated attacker can drop a file that defines a new admin user, which the ServU-FTP will automatically detect. The attacker is then able to log in via FTP and read or replace any file on the server since the FTP server runs with LocalSystem permissions. (CVE-2021-25276)

Successful exploitation of the most severe of these vulnerabilities could result in remote code execution that allows complete control of the underlying Windows operating system. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by SolarWinds to vulnerable systems, immediately after appropriate testing.
- Update Recommendations:
    - Update to SolarWinds Orion Platform Version 2020.2.4
    - Update to SolarWinds ServU-FTP Version 15.2.2 HF1
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
CERT-EU:
https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-008.pdf

ZDNet:
https://www.zdnet.com/article/solarwinds-patches-three-newly-discovered-software-vulnerabilities/

Computer Weekly:

https://www.computerweekly.com/news/252495701/SolarWinds-patches-two-critical-CVEs-in-Orion-platform

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25274
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25275
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25276